

SYHUNT [CODE]

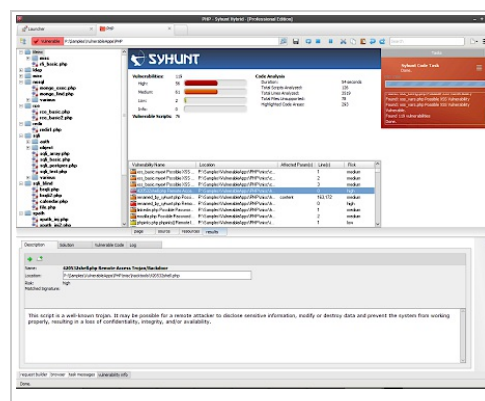


ANALISADOR DE SEGURANÇA DE CÓDIGO-FONTE

Syhunt Code® é a primeira ferramenta comercial amigável e simples de se utilizar capaz de realizar análises profundas do código-fonte de aplicações web. O Syhunt Code torna a vida de desenvolvedores e profissionais de QA (garantia de qualidade) mais fácil através da descoberta automática de múltiplas classes de vulnerabilidades em aplicações web.

CARACTERÍSTICAS PRINCIPAIS

O Syhunt Code permite que desenvolvedores e profissionais de garantia de qualidade (QA) analisem automaticamente qualquer tipo de código-fonte de aplicação por potenciais vulnerabilidades de segurança. O Syhunt Code foi desenvolvido para vasculhar aplicações web por diversos tipos de problemas, como Cross-Site Scripting (XSS), Inclusão de Arquivos, Injeção de SQL, Execução Remota de Comandos e mais. Além disso, através da identificação das principais áreas do código, o Syhunt Code auxilia auditores a realizar revisões de código de maneira melhor, mais veloz e eficiente.



O Syhunt Code é um complemento perfeito para o já extenso conjunto de capacidades para realização de scans de URLs presentes no Syhunt Dynamic, tornando a combinação dos dois produtos na forma do Syhunt Hybrid na solução mais abrangente para aqueles que possuem preocupações em relação a segurança de suas aplicações.

Com o Syhunt Code, você pode:

- Realizar a detecção de mais de **1300** vulnerabilidades de código-fonte, cobrindo mais de 40 tipos de ataques de segurança.
- Realizar o scan do código-fonte de aplicações escritas em ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Lua, Perl, PHP, Python, Ruby (Rails / ERB) e TypeScript em busca por vulnerabilidades.
- Analisar o código-fonte de aplicações web e detectar cross-site scripting, inclusão de arquivos, injeção

de SQL, execução de comandos, problemas de validação e muito mais.

- Identificar áreas chave do código, como tags chave de HTML, JavaScript, requisições XHR, pontos de entrada e palavras-chave interessantes.
- Criar relatórios em HTML e diversos outros formatos - as vulnerabilidades reportadas são por padrão ordenadas com base na pontuação de CVSS3.

Algumas das principais tecnologias suportadas pelo scanner Syhunt Code:



VERIFIQUE POR TODOS OS TIPOS DE VULNERABILIDADES

Verificação	CWE
>_ Execução de Comandos	CWE-78
Injeção de SQL	CWE-89
Injeção de SQL (Funcional)	
Injeção de SQL (Orientada a Objetos)	
Injeção de SQL (Hibernate/HQL)	
Inclusão de Arquivos	CWE-98
Inclusão de Arquivos Locais	
Inclusão de Arquivos Remotos	
Cross-Site Scripting (XSS)	CWE-79
Validação Fraca contra XSS	CWE-79
Pontos de Entrada Ocultos	
Web-Backdoors	
Parâmetros de Depuração	
Injeção de NoSQL	

↪ Redirecionamentos Não Validados	CWE-601
📁 Manipulação de Arquivos Arbitrários	CWE-73
⌘ Divisão de Resposta HTTP	CWE-113
✓ Injeção de LDAP	CWE-90
</> Injeção de Entidades Externas de XML (XXE)	CWE-827
⚠ Injeção de XPath	CWE-643
📄 Falsificação de Solicitação do Lado do Servidor	CWE-918
✓ Forjamento de Log	CWE-117
✓ Divulgação de Informação	CWE-497
✓ Fraquezas Comuns de Formulários	
✓ Hashing Fraco de Senhas	

MICROSOLVED, INC.

“ Identificamos vulnerabilidades significantes com o Syhunt Code. Diversos produtos que revisamos com a ferramenta possuíam várias vulnerabilidades

Brent Huston, CEO,
MicroSolved, Inc.



STEALTH - ISS INC.

“ A melhor ferramenta de auditoria de segurança de aplicações web atualmente no mercado. Rapidamente atualizada para cobrir novas vulnerabilidades e muito fácil de usar.

Robert Davies, CEO, Stealth-
ISS